UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/536,053	03/27/2000	Michael K. Just	0500.9912151	5651

7590 05/25/2004

Markison & Reckamp PC
P O Box 06229
Wacker Drive
Chicago, IL 60606-0229

EXAMINER	
CURCIO, JAMES A F	
ART UNIT	**PAPER NUMBER**
2132	4

DATE MAILED: 05/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/536,053	JUST, MICHAEL K.	
	Examiner	Art Unit	
	James Curcio	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed April 2, 2004 have been fully considered but they are not persuasive.

2. As per claims 1-6, 9-14, 17-25, 28-34, and 37, applicant argues in essence: Chan et al (U.S. 2002/0019941A1) does not appear to determine a digital signature verification error such as verifying a digital signature of a certificate based on a received message header identifier associated with a public key identifier or to generate a digital signature verification map that contains a plurality of acceptable message header identifiers associated with the public key certificate identifier.

However, this argument notwithstanding, Chan et al does disclose the determination of a digital signature verification error based on a received message header identifier associated with a public key certificate identifier (see page 8, second column, third paragraph; page 9, first column, first paragraph; and page 10, first column, second paragraph). The cited sections here include a statement that "the connect () API first checks at step 1202 to see if the calling process 132 is restricted via an appropriate restricted SID in its token 134", and "if not restricted, . . . the connect () API 158 operates as before to return . . . an appropriate errorcode (e.g. no socket available, host unreachable, access denied and so on)".

The Office interprets that checking the SID as per the teaching of this cited section constitutes the determination of a digital signature verification error based on a received message header identifier associated with a public key certificate identifier.

The cited SID ("Security ID") is generated from a binary certificate ID, which the Office interprets to be a part of a certificate containing a digital signature and a received message header identifier. The SID is therefore a received message header identifier associated with a public key certificate identifier, which is in turn directly associated with a digital signature, according to the Office's interpretation. Checking the appropriateness of the restricted SID is therefore equivalent to verifying a digital signature. The cited errorcode returned in the case of a digital signature verification error signifies that the digital signature verification process constitutes the step of determining a digital signature verification error.

Chan et al also discloses the generation of a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier (see page 8, first column, third paragraph and page 9, second column, third and fourth paragraphs). The cited sections state "another way in which to restrict downloaded Internet content is to restrict access to resources based on the site identity. For example, each site has a unique URL (Uniform Resource Locator), and may have a binary certificate ID." The Office interprets that the combination of a unique URL and a binary certificate ID in an SID or another form constitutes a mapping and that multiple such mappings used in determining a digital signature verification error in a manner as described above constitute a digital signature verification map.

3. As per claims 2, 5, 21, 24, 30, and 33, applicant reasserts the relevant remarks made with respect to the relevant independent claims and additionally states in essence: Chan et al (U.S. 2002/0019941A1) does not appear to generate a digital

signature verification map that stores an acceptable message header identifier as a map entry in response to determining the digital signature verification error.

However, this argument notwithstanding, in addition to the teachings cited above, Chan et al discloses the storage, receipt, and digital signature verification map update of at least one acceptable message header identifier, which becomes a map entry (see page 8, first column, third paragraph, last sentence and page 10, first column, first and second paragraphs). The Office interprets the update and storage of the map entry to be a response to determining the digital signature verification error.

4. As per claims 3, 22, and 31, applicant reasserts the relevant remarks made with respect to the relevant independent claims and additionally states in essence: Chan et al (U.S. 2002/0019941A1) does not appear to describe mapping of a plurality of acceptable message header identifiers on a per certificate subject identification basis.

However, this argument notwithstanding, in addition to the teachings cited above, Chan et al does disclose that the generation step includes mapping the plurality of acceptable message header identifiers on a per certificate subject identification basis (see page 8, first column, third paragraph).

5. As per claims 4, 10, 12, 18, 23, 32, applicant reasserts the relevant remarks made with respect to the relevant independent claims and additionally states in essence: Chan et al (U.S. 2002/0019941A1) does not appear to verify a digital signature based on a digital signature verification map.

However, this argument notwithstanding, in addition to the teachings cited above, Chan et al does disclose the verification of a digital signature associated with received

message information based on the digital signature verification map (see page 8, second column, third paragraph; page 9, first column, first paragraph; page 9, second column, third paragraph; and page 10, first column, second paragraph).

6. As per claims 6, 14, 25, and 34, applicant reasserts the relevant remarks made with respect to the relevant independent claims.

However, this reassertion notwithstanding, in addition to the teachings cited above, Chan et al does disclose that the message header identifier includes at least one of data representing a sender's email address, telephone number, and unit identifier (page 8, first column, third paragraph; page 9, second column, second paragraph; and page 9, second column, third paragraph, second sentence).

7. As per claims 9, 11, 13, 19, 28, and 37, applicant argues in essence: Chan et al (U.S. 2002/0019941A1) does not appear to compare a public key certificate identifier with the message header identifier to determine if a mismatch is detected or teach a verification process.

However, this argument notwithstanding, in addition to the teachings cited above, Chan et al does disclose that the determination of a digital signature verification error includes the comparison of a public key certificate identifier with the message header identifier to determine if a mismatch is detected (see "checks at step 1202 to see if the calling process 132 is restricted via an appropriate restricted SID in its token 134" and "the connect () API operates as before to return . . . an appropriate errorcode (e.g., no socket available, host unreachable, access denied, and so on" on page 8, second column, third paragraph), the generation of a mismatch notification for an operator (see

"appropriate error code" on page 8, second column, third paragraph, second sentence), and the verification of a digital signature based on a verification key associated with the public key certificate identifier (See the certificate of the stated message source and SID based on this certificate on page 8, first column, third paragraph; page 8, second column, third paragraph; and page 9, first column, first paragraph. Also see the digital signature of the message that ensures the authenticity of the message source and has a verification key ensured by the above certificate on page 9, second column, third paragraph and page 10, first column, second paragraph.).

8. As per claims 7, 15, 26, and 35, applicant states in essence: Chan et al (U.S. 2002/0019941A1) does not appear to suggest or motivate a step for digitally signing the digital signature verification map to provide a trusted digital signature verification map.

However, this argument notwithstanding, Chan et al does disclose the digital signature of an email message to ensure that the message is trustworthy, that it originates from the trusted message sender listed in the "from" field (see page 9, second column, third paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Chan et al by applying Chan et al's signature technique to the digital signature verification map ("restricted token") containing the acceptable message header identifiers ("restricted SIDs"). One of ordinary skill in the art would have motivated to do in order to ensure that modifications

to the digital signature verification map originate from a trustworthy source (see page 9, second column, third paragraph, second sentence).

9. As per claims 8, 16, 27, 36, 38, and 39, applicant reasserts the relevant remarks made with respect to the Chan reference and additionally argues in essence: Cooper et al (US006052442A) does not appear to contemplate digitally signing or otherwise making an alias map trusted, to provide information security, to employ trusted alias maps, or to provide a trusted alias map containing acceptable message header identifiers in at least one associated subject alias.

In response to applicant's arguments, the recitation "method for providing information security" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See In re Hirao, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and Kropa v. Robie, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

The applicant's additional arguments notwithstanding, in addition to the teachings cited above, Cooper et al, another provider of a verification map containing a plurality of acceptable message header identifiers, does disclose the generation of a trusted alias map containing the plurality of message identifiers and at least one associated subject alias and the display of at least one subject alias (see "directory", "display", and "mnemonic tag" in Cooper et al---page 9, first column, second and sixth paragraphs and

column 10, first paragraph). The Office interprets the directory to be a generated alias map containing the plurality of message identifiers (i.e. "email address") and at least one associated subject alias (i.e. "mnemonic tag") and interprets the display and use of the mnemonic tags to signify that they are trusted.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Chan et al by generating a trusted alias map relating Chan et al's URLs or sender email addresses to corresponding mnemonic aliases and by displaying these aliases in place of the same URLs and sender email addresses. One of ordinary skill in the art would have been motivated to do so in order to facilitate the identification of Chan et al's message sources.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-6, 9-14, 17-25, 28-34, and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by Chan et al (US20020019941A1).

12. As per claims 1, 17, 20, and 29, Chan et al discloses the determination of a digital signature verification error (see page 8, second column, third paragraph; page 9, first column, first paragraph; and page 10, first column, second paragraph) and the

generation of a digital signature verification map (see page 8, first column, third paragraph and page 9, second column, third and fourth paragraphs).

13. As per claims 2, 5, 21, 24, 30, and 33, in addition to the teachings applied above, Chan et al discloses the storage, receipt, and digital signature verification map update of at least one acceptable message header identifier, which becomes a map entry (see page 8, first column, third paragraph, last sentence and page 10, first column, first and second paragraphs).

14. As per claims 3, 22, and 31, in addition to the teachings applied above, Chan et al discloses that the generation step includes mapping the plurality of acceptable message header identifiers on a per certificate subject identification basis (see page 8, first column, third paragraph).

15. As per claims 4, 10, 12, 18, 23, and 32, in addition to the teachings applied above, Chan et al discloses the verification of a digital signature associated with received message information (see page 8, second column, third paragraph; page 9, first column, first paragraph; page 9, second column, third paragraph; and page 10, first column, second paragraph).

16. As per claims 6, 14, 25, and 34, in addition to the teachings applied above, Chan et al discloses that the message header identifier includes at least one of data representing a sender's email address, telephone number, and unit identifier (page 8, first column, third paragraph; page 9, second column, second paragraph; and page 9, second column, third paragraph, second sentence).

17. As per claims 9, 11, 13, 19, 28, and 37, in addition to the teachings applied above, Chan et al discloses that the determination of a digital signature verification error includes the comparison of a public key certificate identifier with the message header identifier (see page 8, second column, third paragraph), the generation of a mismatch notification (see "appropriate error code" on page 8, second column, third paragraph, second sentence), and the verification of a digital signature based on a verification key associated with the public key certificate identifier (See the certificate of the stated message source and SID based on this certificate on page 8, first column, third paragraph; page 8, second column, third paragraph; and page 9, first column, first paragraph. Also see the digital signature of the message that ensures the authenticity of the message source and has a verification key ensured by the above certificate on page 9, second column, third paragraph and page 10, first column, second paragraph.).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 7, 15, 26, and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al (US20020019941A1). Chan et al discloses the determination of a digital signature verification error (see page 8, second column, third paragraph; page 9, first column, first paragraph; and page 10, first column, second paragraph) and the generation of a digital signature verification map (see page 8, first column, third

paragraph and page 9, second column, third and fourth paragraphs). Chan et al also discloses the storage, receipt, and digital signature verification map update of at least one acceptable message header identifier, which becomes a map entry (see page 8, first column, third paragraph, last sentence and page 10, first column, first and second paragraphs). Chan et al additionally discloses the verification of a digital signature associated with received message information (see page 8, second column, third paragraph; page 9, first column, first paragraph; page 9, second column, third paragraph; and page 10, first column, second paragraph). Chan et al also discloses that the determination of a digital signature verification error includes the comparison of a public key certificate identifier with the message header identifier (see page 8, second column, third paragraph), the generation of a mismatch notification (see "appropriate error code" on page 8, second column, third paragraph, second sentence), and the verification of a digital signature based on a verification key associated with the public key certificate identifier (See the certificate of the stated message source and SID based on this certificate on page 8, first column, third paragraph; page 8, second column, third paragraph; and page 9, first column, first paragraph. Also see the digital signature of the message that ensures the authenticity of the message source and has a verification key ensured by the above certificate on page 9, second column, third paragraph and page 10, first column, second paragraph.).

Chan et al fails to expressly disclose the digital signature of the digital signature verification map. However, Chan et al does disclose the digital signature of an email

message to ensure that the message is trustworthy, that it originates from the trusted message sender listed in the "from" field (see page 9, second column, third paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Chan et al by applying Chan et al's signature technique to the digital signature verification map ("restricted token") containing the acceptable message header identifiers ("restricted SIDs"). One of ordinary skill in the art would have motivated to do in order to ensure that modifications to the digital signature verification map originate from a trustworthy source (see page 9, second column, third paragraph, second sentence).

20. Claims 8, 16, 27, 36, 38, and 39 rejected under 35 U.S.C. 103(a) as being unpatentable over Chan et al (US20020019941A1) as applied to claims 1, 10, 20, and 29 above, and further in view of Cooper et al (US006052442A). Chan et al discloses the determination of a digital signature verification error (see Chan et al---page 8, second column, third paragraph; page 9, first column, first paragraph; and page 10, first column, second paragraph) and the generation of a digital signature verification map (see Chan et al---page 8, first column, third paragraph and page 9, second column, third and fourth paragraphs). Chan et al also discloses the storage, receipt, and digital signature verification map update of at least one acceptable message header identifier, which becomes a map entry (see Chan et al---page 8, first column, third paragraph, last sentence and page 10, first column, first and second paragraphs). Chan et al additionally discloses the verification of a digital signature associated with received message information (see Chan et al---page 8, second column, third paragraph; page 9,

first column, first paragraph; page 9, second column, third paragraph; and page 10, first column, second paragraph).

Chan et al fails to expressly disclose the generation of a trusted alias map and the display of at least one subject alias. However, Cooper et al discloses these features (see "directory", "display", and "mnemonic tag" in Cooper et al---page 9, first column, second and sixth paragraphs and column 10, first paragraph).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Chan et al by generating a trusted alias map relating Chan et al's URLs or sender email addresses to corresponding mnemonic aliases and by displaying these aliases in place of the same URLs and sender email addresses. One of ordinary skill in the art would have been motivated to do so in order to facilitate the identification of Chan et al's message sources.

Conclusion

21. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Curcio whose telephone number is 703-305-8887. The examiner can normally be reached on Tuesday through Friday from 7:00 am – 5:30 pm.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached at 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

24. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

JC
AU 2132
May 18, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100